Issues in Software System Safety:

Polly Ann Smith Co.
v.
Ned I. Ludd

C. Michael Holloway

Presented at the 20th International System Safety Conference
Denver, Colorado
August 5-9, 2002

Langley Research Center

Disclaimers

- This is a work of fiction, although I will pretend it is real
  - The case is not real
  - The accident giving rise to the case is not real
  - The people are not real (with a few obvious exceptions)
  - The software techniques mentioned are not real
  - The cited precedence cases and federal rules *are real*
- I am not a lawyer, nor do I play one on TV
  - This is not expert legal commentary
  - Several simplifications have been made
- My goal is to stimulate friendly discussion about a few issues over which discussion is often not so friendly

Outline

- Description of the case
  - Facts
  - Initial Litigation
  - Ruling by District Court
  - Ruling by Circuit Court
  - Ruling by Grand Court
- Group discussion of the issues raised by the case
  - What is truly known about software system engineering, especially for safety-critical systems?
  - Are there software engineering experts? If so, what are their qualifications?
  - What constitutes proof of software engineering principles, tools, and techniques, especially when system safety is at risk?

The Facts of the Case

- Ludd was injured in crash of a small aircraft he was piloting
  - Low-visibility landing attempt using automated landing system named Amelia, which was built by the Polly Ann Smith Company
  - Crashed short of the runway
  - Ludd survived the crash, but sustained serious injuries, which left him partially disabled
- Investigation uncovered erroneous software in Amelia
  - Under certain meteorological and geographic conditions, Amelia sent wrong commands to control surfaces
  - Unless overridden by pilot, these commands would cause aircraft to contact the ground several hundred feet short of the runway threshold

Litigation Begins

- Ludd sued Polly Ann Smith Company
  - Alleging negligence in design and implementation of Amelia
  - For failing to apply state-of-the-practice software safety techniques to the design and assessment of the system
- Case rested primarily on depositions of G. Clarke, an internationally-recognized software safety researcher,who was prepared to testify that
  - Certain software safety principles represent the current state-of-the-practice
  - Smith's knowledge of these principles was deficient
  - Records showed no application of these principles in the creation and deployment of the Amelia software

Smith Responds

- Polly Ann Smith Co. did not contest that Amelia software contributed to Ludd's accident, but denied negligence
- Moved to exclude Clarke's proffered testimony because
  - (1) he didn't qualify as an expert witness, or
  - (2) his opinions on the deficiencies in Amelia development did not rise above 'subjective belief or unsupported speculation'*
- Further moved for summary judgment in its favor on the grounds that without Clarke's testimony Ludd did not have any evidence to support his claim of negligence

* *General Electric, Co. v. Joiner*, 522 U.S. 136 (1997)

Smith's Basis for Motions

- On its behalf, Smith offered depositions from its own expert, C. Vantile, an internationally-recognized software researcher, and developer of widely-used techniques for analyzing the correctness of software systems
- Vantile planned to testify that
  - Software safety principles did not represent the state-of-the-practice
  - The true state-of-the-practice was represented by the application of his own techniques for software assurance
  - Smith had applied these techniques in developing Amelia
  - No one could have been expected to discover the flaws in Amelia that led to Ludd's accident

The District Court Rules

- Granted Smith's motion to exclude Clarke's testimony and entered summary judgment for Smith
- Based its ruling on
  - Court's obligation to ensure that proposed expert testimony is both relevant and reliable
  - Clarke's testimony failed the appropriate tests for reliability of the underlying methods upon which it was based, and thus must be excluded
  - Without Clarke's testimony, Ludd had no evidence of negligence by Smith
- Ludd appealed

The Circuit Court Overturns

- Circuit Court asserted that the District Court had abused its discretion in excluding Clarke's testimony
  - Clarke's credentials as an expert were impeccable
    - International reputation
    - Numerous published papers
    - Consultant to companies and government agencies
  - Disallowing such a person's testimony was, on its face, abuse of discretion
- Smith appealed, and the Grand Court agreed to hear the case

The Grand Court Rules

- By a 6-3 decision, the Grand Court
  - Affirmed that the District Court erred in excluding Clarke's testimony
  - Said the Circuit Court's rationale for its judgment was wrong
- Opinion of the court
  - Reaffirmed principle of distinguishing between qualification as an expert and allowing particular testimony
  - Distinguished between 'gatekeeper' and 'arbiter' roles
- Dissenting opinion
  - Agreed with majority's distinctions in principle, but dissented from the application of these distinctions in this case
  - Asserted that neither Clarke's nor Vantile's testimony should have been allowed

Opinion of the Court

- General Observations
  - "Abuse of discretion is the appropriate standard of review."
  - "Federal Rule of Evidence 702 is controlling in this case: 'If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case'."

Opinion of the Court (continued)

- Expert witnesses in this case
  - "Without question, 'scientific, technical, or other specialized knowledge' is necessary 'to understand the evidence' in this case. Thus, the use of expert witnesses is warranted."
  - "Also without question, Ludd's proffered expert witness, G. Clarke, 'qualified as an expert by knowledge, skill, experience, training, or education'. So, too, did C. Vantile, Smith's proffered expert."
  - "Had the District Court failed to qualify either person as an expert, it would have abused its discretion. But the Court did not exclude them as experts; instead, it excluded Clarke's specific testimony as being neither 'based upon sufficient facts or data', nor 'the product of reliable principles and methods.' We must determine whether *that* exclusion was an abuse of discretion."

Opinion of the Court (continued)

- Excluding Clarke's testimony was abuse of discretion
  - "A trial court has wide discretion in determining how to test the reliability of the principles and methods upon which testimony is based; however, this 'is not discretion to perform the function inadequately. Rather, it is discretion to choose among *reasonable* means of excluding expertise that is *fausse* and science that is junky.'*"
  - "The means chosen by the District Court was not reasonable, however, as we now show."

* *Kumho Tire Col., Ltd., et al. v. Carmichael et al.*, 526 U.S. 137 (1999), J. Scalia, concurring

Opinion of the Court (continued)

- The District Court's determination "presumes too much in asserting that there exist only two means of showing reliability: controlled experiments and logical proof.
  - There are other means, such as case studies, quasi-experiments, and rigorous (although not strictly formally sound) reasoning.
  - Clarke's testimony cited examples of the use of these methods to support his contentions."

Opinion of the Court (continued)

- "The ruling also presumes too much in assuming that a court is an appropriate arbiter between conflicting theories in technical fields."
  - "The court has determined what the professional community of which Vantile and Clarke are members has not been able to determine: namely, that one of these internationally acclaimed men is wrong (Clarke), and the other is right (Vantile).
  - To make this determination, the court has become the 'amateur scientists' against which we were warned. *
  - This is not only abuse of discretion; it is arrogance of the highest (or should that be, lowest) order."

* *Daubert, et al. v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), CJ. Rehnquist, concurring in part and dissenting in part.

Opinion of the Court (continued)

- "The Circuit Court was right to overturn the District Court's ruling, but it was wrong in its reasoning. We affirm the judgment, but remand the case to the District Court for further proceedings consistent with this opinion."

Dissenting Opinion

- "We agree with much of what the majority has to say. Abuse of discretion is the right standard of review. *If* we agreed that Rule 702 applied in this case, we probably would concur with the analysis presented by our distinguished colleagues.
  - However, the most beautiful edifice will not long stand if it is built upon a foundation of quicksand; the Court's analysis cannot stand, because it is built on nothing more substantial than quicksand.
  - The foundation is quicksand because Rule 702 does not apply."

Dissenting Opinion (continued)

- "For Rule 702 to apply, there must exist 'scientific, technical, or other specialized knowledge' relevant to the case.
  - The Court believes that such knowledge about software development practices exists in this case.
  - We believe the Court has confused 'knowledge' with 'opinion'. The two do not mean the same thing, as any dictionary will show."

Dissenting Opinion (continued)

- "There is no question that a substantial body of literature exists about every aspect of software engineering, including the description of various methods for ensuring the safety of software used in critical applications. G. Clarke and C. Vantile have made numerous contributions to this literature. …"

- "[W] hen reviewing representative publications from this body of literature, including papers by both Clarke and Vantile, one cannot help but be struck by the extent to which these publications contain little more than '*belief[s] or conclusion[s] held with confidence but not substantiated by positive knowledge or proof*' (that is, opinion)."

Dissenting Opinion (continued)

- "Even more striking is the way in which quite a few people, Clarke and Vantile included, appear to start off their publishing careers acknowledging the basic lack of knowledge in the field.
  - As time goes on, these people, Clarke and Vantile included, make increasingly dogmatic statements, without any increase in the quantity or quality of the evidence given to support these statements.
  - The clear impression is that many people, Clarke and Vantile included, come to deceive themselves into believing they have knowledge, when all they really have is opinion."

- "To put it bluntly, to assert that there exists software engineering 'knowledge' is to strip the word 'knowledge' of any distinction from mere opinion."

Dissenting Opinion (continued)

- "The Court writes, 'It is only slightly hyperbolic to say that, if Clarke and Vantile are not experts in the field, there are no experts in the field.' Under the meaning of 'expert' in Rule 702, neither Clarke nor Vantile nor anyone else in the field is a software engineering expert, because there is no "scientific, technical, or other specialized knowledge" in software engineering in which to be an expert.

- It is only slightly hyperbolic to say that in software engineering, all expertise is *fausse* and all science is junky.

- Perhaps one day there will exist 'knowledge' in software engineering, but that day is not today."

Dissenting Opinion (continued)

- “For the reasons given above, we respectfully dissent.
- The District Court did not abuse its discretion when it disallowed Clarke’s testimony.
- We would reverse the ruling of the Circuit Court.
- We would also note that the issue of whether to allow Vantile’s testimony became mute when the District Court ruled that, with Clarke’s testimony excluded, Ludd did not have a case. Had the issue not been mute, Vantile’s testimony should also have been excluded, for the same reason as Clarke’s testimony should be excluded.

Paraphrase of Opinions

- Majority
  - Both Clarke and Vantile possess ‘scientific, technical, or other specialized knowledge’ relevant to the case
  - In disallowing Clarke’s testimony, the District Court improperly assumed the role of arbiter of a professional dispute in which *both sides have reasonable evidence for their positions*
- Dissent
  - Neither Clark nor Vantile possess ‘scientific, technical, or other specialized knowledge’
  - *All that either has is opinion without reasonable evidence to support the opinion*

Time to Vote

- Before we begin discussion, we'll take a vote.
- From the following propositions, choose the one that most closely represents your opinion about this case:
  - I **strongly agree** with the **majority** opinion
  - I agree **more** with the **majority** than the dissent
  - I agree **more** with the **dissent** than with the majority
  - I **strongly agree** with the **dissenting** opinion
  - I **strongly disagree with both** of them
- Does anyone have any clarifying questions to ask before voting?

Let the Discussion Begin!

What is truly known about software system engineering,
especially for safety-critical systems?

Are there software engineering experts?
If so, what are their qualifications?

What constitutes proof of software engineering principles,
tools, and techniques,
especially when system safety is at risk?